State of Arkansas
Office of Information Technology
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Agency # 200.00

DRAFT Standard Statement – Remote Access

Title: Remote Access

Document Number: SS-70-009

Effective Date: x/x/2007

Published by: Office of Information Technology

1.0 Purpose

There are many instances when authorized individuals require remote access to sensitive state information technology resources. Examples of remote access include, but are not limited to, employees checking email while traveling, inspectors submitting reports from the field, and contractors accessing machines to troubleshoot problems. In many cases, these individuals are using personally-owned computing devices to gain access to state resources which could introduce these resources to cyber infection. Access to the state network and the state's sensitive information technology resources should be regulated to ensure effective protection measures are in place to minimize the risk of compromise.

2.0 Scope

This standard statement applies to all state agencies, administrative portions of institutions of higher education, boards and commissions.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies, boards and commissions and administrative portions of institutions of higher education.

4.0 References

4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.

4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

5.1 Remote access of non-publicly available state information technology resources by state employees or authorized entities shall comply with the following requirements:

5.1.1 Spyware Scanning Standard (SS-70-005)
5.1.2 Virus Scanning Standard (SS-70-004)

5.1.3 The client operating system and Internet browser patch levels must be current.

5.1.4 The client operating system and Internet browser versions must be currently supported by the manufacturer.

5.2 Agency email accessed from outside the agency shall utilize web access technologies that encrypt the communications from the client to the email server.

5.3 Remote access of Level B (Sensitive), Level C (Very Sensitive) and Level D (Extremely Sensitive) data, classified by the Data and System Security Classification Standard (SS-70-001), housed by covered entities, must utilize secure virtual private network (VPNs).

5.4 Split tunnel VPNs, unencrypted VPNs and https servers shall be configured to disallow general file access to Level B, Level C and Level D data.

5.5 Applications allowing controlled access to specific records containing Level B, Level C and Level D data may utilize split tunneling technologies and/or the https protocol.

5.6 All methods of encryption utilized during remote access must comply with the Encryption Standard (SS-70-006).

6.0 Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception or exclusion to any part of this standard.

7.0 Revision History

Date	Description of Change
x/x/2007	Original Standard Statement Published

8.0 Definitions

8.1 Remote Access

Remote access is the ability to get access to a computer or a network from outside the organization through the use of an electronic device.

8.2 Secure Virtual Private Network (VPN)

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses. Secure VPNs do not allow split tunneling.

8.3 Split Tunneling

The process of allowing a remote VPN user access a public network, most commonly the Internet, at the same time that the user is allowed to access resources on the VPN. This method of network access enables the user to access remote devices, such as a networked printer, at the same time as accessing the public network. An advantage of using split tunneling is that it alleviates bottlenecks and conserves bandwidth as Internet traffic does not have to pass through the VPN server. A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network.

9.0 Related Resources

9.1 Data and System Security Classification Standard (SS-70-001): http://www.cio.arkansas.gov/techarch/indexes/standards.htm

9.2 Encryption Standard (SS-70-006): http://www.cio.arkansas.gov/techarch/indexes/standards.htm

9.3 COBIT standards: www.isaca.org/cobit.htm

9.4 Physical and Logical Security Standard (SS-70-008): http://www.cio.arkansas.gov/techarch/indexes/standards.htm

10.0 Inquiries

Direct inquiries about this standard to:

Office of Information Technology
Shared Technical Architecture
124 West Capitol Avenue Suite 990, Little Rock, Arkansas 72201
Phone: 501-682-4300
FAX: 501-682-2040
Email: sharedarchitecture@arkansas.gov

OIT standards, policies and best practices can be found on the Internet at: http://www.cio.arkansas.gov/techarch